## ANEXO IV

## REGULAMENTO DOS REQUISITOS PARA PRESTADORES QUALIFICADOS DE SERVIÇOS DE CONFIANÇA

## PREÂMBULO

A Agência Reguladora Multissectorial da Economia – ARME, nos termos do n.º 1, do artigo 1.º, do Decreto-lei n.º 50/2018, de 20 de setembro, que cria a ARME e aprova os seus Estatutos, é uma autoridade administrativa independente, de base institucional, dotada de funções reguladoras, incluindo a de regulamentação, supervisão e sancionamento de infrações, que tem por finalidade principal a atividade administrativa de regulação técnica e económica dos setores das comunicações eletrónicas, energia, água e transportes coletivos urbanos e interurbanos de passageiros, segundo o n.º 1, do artigo 2.º, do Decreto-lei n.º 50/2018, de 20 de outubro.

O Decreto-lei n.º 50/2018, de 20 de setembro, na alínea *f)*, do seu artigo 15.º, atribui aos órgãos da ARME, no âmbito da sua competência de supervisão, como entidade reguladora do setor das comunicações eletrónicas, a competência de supervisionar as entidades de certificação.

Assim, definiu-se no artigo 82.º, do Decreto-lei n.º 27/2023, de 20 de outubro, que estabelece as normas aplicáveis aos serviços de confiança, nomeadamente às transações eletrónicas, e institui um quadro legal para as assinaturas eletrónicas, os selos eletrónicos, os selos temporais, os documentos eletrónicos, os serviços de certificados para autenticação de sítios *Web,* arquivo eletrónico, o certificado eletrónico de atributos, a gestão de dispositivos de criação de assinaturas e de selos eletrónicos à distância, e os livros-razão eletrónicos, que as funções de autoridade credenciadora são atribuídas à Entidade Reguladora do Sector das Comunicações Eletrónicas, ou seja, à ARME.

Para a prossecução destas atribuições, no âmbito da sua competência como Entidade Reguladora do Sector das Comunicações Eletrónicas, incluindo, principalmente, as funções como autoridade credenciadora, a ARME deve emitir e publicar no seu sítio da *Internet* e no *Boletim Oficial* as regras de técnicas e de segurança aplicáveis ao exercício da atividade de prestação de serviço de confiança, nos termos do artigo 99.º, do Decreto-Lei n.º 27/2023, de 20 de outubro.

O artigo 3.º, do Decreto-lei n.º 23/2023, de 20 de outubro define os prestadores qualificados de serviços de confiança como entidades que fornecem um ou mais dos seguintes serviços de criação, verificação e validação de assinaturas eletrónicas, selos eletrónicos ou selos temporais, serviços de envio registado eletrónico e certificados relacionados com estes serviços; criação, verificação e validação de certificados para a autenticação de sítios *web*; conservação das assinaturas, selos ou certificados eletrónicos relacionados com esses serviços; arquivo eletrónico de documentos eletrónicos; gestão de dispositivos de criação de assinaturas e de selos eletrónicos à distância; registo de dados eletrónicos num livro-razão eletrónico.

Um prestador de serviços de confiança para prestar os serviços suprarreferidos, no âmbito da Infraestrutura de Chaves Públicas de Cabo Verde – ICP – CV, é necessário que a Autoridade Credenciadora lhe atribua o estatuto de prestador qualificado de serviços de confiança, mediante procedimento que se inicia com o pedido de atribuição do estatuto de prestador qualificado de serviços de confiança, nos termos do artigo 25.º, do Decreto-lei n.º 27/2023, de 20 de outubro.

O estatuto de prestador qualificado de serviços de confiança é atribuído pela autoridade credenciadora e pressupõe que os prestadores de serviços de confiança satisfaçam os seguintes requisitos legais presentes no artigo 26.º, do Decreto-lei n.º 27/2023, de 20 de outubro. Uma vez atribuído, tem a duração de três anos e poder ser renovado por igual período, consoante o n.º 7, do artigo 25.º, do Decreto-lei n.º 27/2023, de 20 de outubro, ou revogado, nos termos do artigo 31.º, do Decreto-lei n.º 27/2023, de 20 de outubro.

Neste sentido, o Regulamento dos Requisitos para Prestadores Qualificados de Serviços de Confiança tem por objeto definir as condições de elegibilidade de prestadores de serviços de confiança, para obterem e manterem o estatuto de qualificados no âmbito do Decreto-lei n.º 27/2023 de 20 de outubro, e de acordo com as seguintes normas internacionais de referência aplicadas às atividades de certificação e credenciação, ETSI EN 319 401; ETSI EN 319 411-1; ETSI EN 319 411-2; ETSI EN 319 412-1; ETSI EN 319 412-2; ETSI EN 319 412-3; ETSI EN 319 412-4; ETSI EN 319 412-5; ETSI EN 319 421; ETSI EN 319 422; ETSI TS 119 431-1; ETSI TS 119 431-2; ETSI TS 119 432; ETSI TS 119 441; ETSI TS 119 442; ETSI TS 119 511; ETSI TS 119 512; ETSI EN 319 521; ETSI EN 319 522; ETSI EN 319 531; ETSI EN 319 532; ETSI TR 102 044; ETSI TS 102 158; ETSI TS 119 101; ETSI TS 119 312; ETSI TS 119 431-1; ETSI TS 119 431-2; ETSI TS 119 432; IETF RFC 3647; ISO/IEC 15408 (parts 1 to 3); ISO/IEC 19790; ETSI EN 319 102-1; ETSI TS 119 102-2; e ETSI TS 119 172-4.

Artigo 1.º

**Objeto**

O presente regulamento define as condições de elegibilidade de prestadores de serviços de confiança, para obterem e manterem o estatuto de qualificados, no âmbito do Decreto-lei n.º 27/2023 de 20 de outubro.

Artigo 2.º

**Âmbito**

O presente regulamento aplica-se a prestadores de serviços de confiança que desejam obter ou renovar o estatuto de prestador qualificado de um ou mais serviços definidos no Decreto-lei n.º 27/2023, de 20 de outubro.

Artigo 3.º

**Siglas**

No presente regulamento são utilizadas as seguintes siglas:

a) ARME: Agência Reguladora Multissetorial da Economia;

b) DPC: Declaração de Práticas de Certificação;

c) ETSI: European Telecommunications Standards Institute;

d) FIPS PUB: Federal Information Processing Standard Publications;

e) HSM: Hardware Security Module;

f) ISO/IEC: International Organization for Standardization / International Electrotechnical Commission;

g) PC: Política de Certificação;

h) PCN: Plano de Continuidade de Negócios;

i) PQSC: Prestador Qualificado de Serviços de Confiança

j) PSC: Prestador de Serviços de Confiança;

k) QSCD: Dispositivos Qualificados de Criação de Assinaturas/Selos Eletrônicos;

l) RFC: Request for Comments.

Artigo 3.º

**Requisitos para prestadores qualificados de serviços de confiança**

1. Os prestadores de serviços de confiança que desejam fornecer os serviços qualificados devem proceder à sua credenciação junto da autoridade credenciadora.

2. Os prestadores de serviços de confiança devem preencher o formulário Pedido de Credenciação de Prestador Qualificado de Serviços de Confiança disponível no *website* da autoridade credenciadora e apresentar a documentação e os comprovativos definidos no Decreto-lei n.º 27/2023, de 20 de outubro.

3. Os prestadores de serviços de confiança, para obter o estatuto de qualificados, devem, ainda, assegurar que as suas instalações, procedimentos, atributos de pessoal, equipamentos e sistemas obedecem às normas de segurança aplicáveis ao exercício da sua atividade, preenchendo os seguintes requisitos:

   *a)* Estabelecer ou adaptar a sua atividade operacional de acordo com os requisitos definidos no Decreto-lei n.º 27/2023, de 20 de outubro, e nos documentos presentes na tabela, no anexo parte integrantes deste documento;

   *b)* Elaborar uma Declaração de Práticas para cada tipo de serviço prestado, com o objetivo de informar os usuários e terceiras partes como o prestador organiza e executa suas atividades, bem como informar detalhes sobre os serviços de confiança prestados;

   *c)* Tratando-se de um prestador de serviço de confiança que emite certificados digitais qualificados, deve elaborar uma Declaração de Práticas de Certificação e uma Política de Certificação:

      *i.* A Declaração de Práticas de Certificação deve necessariamente observar a estrutura definida na IETF RFC 3647 e descrever os processos que o prestador do serviço usará na criação e manutenção do certificado.

      *ii.* A Política de Certificação deve referir os tipos de certificados que o prestador emite, de acordo com a norma ETSI 319 411-2 e descrever cada tipo em termos de qualidade;

      *iii.* A Política de Certificação pode ser um documento autónomo ou ser fornecido como parte da Declaração de Práticas de Certificação.

      *iv.* Os documentos referidos substituem a Declaração de Práticas referida em relação ao fornecimento de certificados digitais.

      *v.* Caso o prestador ofereça também outros serviços, deve elaborar uma Declaração de Práticas para cada um dos demais serviços prestados.

   *d)* Elaborar o Plano de Segurança, previsto no artigo 25.º do Decreto-lei n.º 27/2023, de 20 de outubro, em conformidade com o descrito na norma ISO/IEC 27001 e com os requisitos descritos no artigo 6.º;

*e)* Efetuar uma Avaliação de Riscos, em conformidade com o descrito no documento ETSI EN 319 401 e na norma ISO/IEC 27005, que deve ser levada ao conhecimento do órgão executivo do prestador de serviços para conhecimento e assinatura;

*f)* Elaborar e manter um Inventário de todos os ativos de informação, atribuindo uma classificação consistente com a avaliação de risco, em conformidade com o descrito na norma ISO/IEC 27002, que deve ser atualizado sempre que houver alterações nos ativos e conferido no mínimo anualmente.

*g)* Elaborar um Plano de Contingência, que contenha, no mínimo, os requisitos descritos no artigo 7.º;

*h)* Elaborar uma Política de Pessoal, responsável pelas funções de gestão dos serviços de confiança, que contenha, no mínimo, os requisitos descritos no artigo 8.º.

*i)* Elaborar um Plano de Encerramento que contenha, no mínimo, os requisitos descritos no artigo 9.º.

*j)* Utilizar Sistemas e Dispositivos Fiáveis, de acordo com o disposto no artigo 10.º.

*k)* Desenvolver a atividade em instalações físicas adequadas, em conformidade com os requisitos definidos no Regulamento de segurança física de instalações de prestadores qualificados de serviços de confiança;

*l)* Se o prestador de serviços fizer emissão de certificados digitais, as respetivas atividades de registo devem ser executadas em ambiente físico;

*m)* Contratar os serviços de um Organismo de Avaliação de Conformidade credenciado pela autoridade credenciadora, para realização de auditoria pré-operacional, para fins de obtenção do estatuto de Prestador Qualificado de Serviços de Confiança, e auditoria operacional anual, para fins de manutenção do estatuto de qualificado, conforme definido no Regulamento de avaliação de conformidade.

Artigo 4.º

**Pedido de credenciação**

1. O candidato a prestador qualificado de serviços de confiança, para iniciar o processo de credenciação inicial, deve encaminhar à ARME os seguintes documentos:

   *a)* Pedido de Credenciação de Prestador Qualificado de Serviços de Confiança;

   *b)* Estatutos da pessoa coletiva e, tratando-se de sociedade, contrato de sociedade;

   *c)* Tratando-se de sociedade, relação de todos os sócios, com especificação das respetivas participações, bem como dos membros dos órgãos de administração e de fiscalização,

e, tratando-se de sociedade anónima, relação de todos os acionistas com participações significativas, diretas ou indiretas;

*d)* Declarações subscritas por todas as pessoas singulares e coletivas de que não se encontram em nenhuma das situações indiciadoras de falta de idoneidade;

*e)* Prova do substrato patrimonial e dos meios financeiros disponíveis, designadamente da realização integral do capital social;

*f)* Descrição da organização interna e plano de segurança;

*g)* Demonstração dos meios técnicos e humanos exigidos pela autoridade credenciadora, incluindo certificados de conformidade dos produtos de serviços de confiança emitidos por organismos de certificação;

*h)* Programa geral da atividade prevista para os primeiros três anos;

*i)* Descrição geral das atividades exercidas nos últimos três anos ou no tempo decorrido desde a constituição, se for inferior, e balanço e contas dos exercícios correspondentes;

*j)* Comprovação de contrato de seguro válido para cobertura adequada da responsabilidade civil emergente da atividade de certificação.

*k)* Os documentos técnicos referidos do n.º 3, do artigo 3.º;

*l)* Relatório da auditoria pré-operacional que contemple a avaliação de conformidade de todos os serviços para os quais esteja solicitando o estatuto de qualificado.

4. Os documentos são analisados pela autoridade credenciadora, que tomará a decisão de aceitar ou recusar o pedido do estatuto de qualificado de serviços de confiança.

5. O estatuto de prestador qualificado de serviços de confiança é válido pelo período de 3 anos, podendo ser objeto de renovação por períodos de igual duração.

Artigo 5.º

**Renovação da credenciação**

1. O prestador qualificado de serviços de confiança, para iniciar o processo de renovação da credenciação, deve encaminhar à autoridade credenciadora os seguintes documentos:

*a)* Pedido de Renovação de Credenciação de Prestador Qualificado de Serviços de Confiança, conforme formulário disponível no sítio da autoridade credenciadora;

*b)* Atualização dos documentos referidos no n.º 1, do artigo 4.º;

*c)* Atualização dos documentos técnicos definidos no n.º 3, do artigo 3.º;

*d)* Relatório de auditoria operacional que contemple a última avaliação de conformidade de todos os serviços para os quais esteja solicitando a renovação do estatuto de qualificado.

2. Os documentos apresentados são analisados pelos órgãos competentes da autoridade credenciadora, podendo o pedido de renovação do estatuto de prestador qualificado de serviços de confiança ser aceite ou recusada.

Artigo 6.º

**Plano de segurança**

1. O Prestador Qualificado de Serviço de Confiança deve elaborar um Plano de Segurança que contemple, no mínimo, as seguintes informações:
   *a)* Descrição da estrutura organizacional e funcional e da atividade de serviços de confiança que é prestada;
   *b)* Especificação dos processos de avaliação e de garantia da idoneidade e capacidade técnica do pessoal em funções;
   *c)* Especificação dos requisitos de segurança física, lógica e operacional;
   *d)* Requisitos de disponibilidade da informação, incluindo redundância de sistemas e planos de contingência;
   *e)* Requisitos de proteção da informação, incluindo distinção dos vários níveis de segurança e perfis de acesso implementados;
   *f)* Definição das funções que conferem acesso aos atos e instrumentos dos serviços de confiança, respetivos requisitos de segurança e perfis de acesso;
   *g)* Descrição dos produtos de assinatura eletrónica utilizados e identificação das respetivas certificações de conformidade, quando aplicável;
   *h)* Descrição e avaliação de outros riscos de segurança;
   *i)* Indicação dos responsáveis pela sua implementação;
   *j)* Indicação do processo de revisão periódica estabelecido.
2. A equipa que atua diretamente nos serviços de confiança deve ser formalmente informada sobre a existência e conteúdo do Plano de Segurança.

Artigo 7.º

**Plano de contingência**

1. O prestador qualificado de serviços de confiança, para fazer face à eventual ocorrência de desastres ou incidentes que ponham em causa o funcionamento normal dos serviços prestados, deve dispor de procedimentos que permitam a continuação dos serviços em sistemas de recuperação alternativos e garantam que a migração dos sistemas primários para os sistemas de recuperação não põe em risco a segurança dos sistemas.
2. No caso do prestador de serviço de emissão de certificados e selos digitais, deve ser assegurado que os serviços de distribuição, revogação e estado de revogação de certificados se mantêm permanentemente disponíveis mesmo em caso de incidentes.

3. O prestador qualificado de serviços de confiança deve implementar um Plano de Continuidade de Negócios, que contemple, no mínimo:

   a) a possibilidade de adulteração ou acesso não autorizado às chaves privadas próprias ou de terceiros sob sua custódia, quando aplicável;

   b) a invasão de seus sistemas e da rede interna;

   c) incidentes de segurança física e lógica;

   d) indisponibilidade da infraestrutura;

   e) fraudes ocorridas no registo do utilizador, na emissão, expedição, distribuição, revogação e gestão de certificados, caso se trate de prestador qualificado de serviços de confiança que emita certificados digitais.

4. O Plano de Continuidade de Negócios deve conter os seguintes procedimentos:

   a) retoma das operações em espaço de tempo que cause o mínimo impacto possível aos usuários;

   b) notificação aos requerentes, titulares, destinatários e outras entidades com as quais exista acordo, sobre qualquer acontecimento que ponha em causa a utilização segura dos serviços que oferece;

   c) notificação às autoridades, se for o caso;

   d) revogação dos certificados afetados, se for o caso;

   e) procedimentos para interrupção ou suspensão de serviços e investigação do incidente;

   f) análise e monitorização de registos de auditoria; e

   g) relacionamento com o público e com meios de comunicação, se for o caso.

5. Todos os envolvidos com o Plano de Continuidade de Negócios devem receber formação específica para enfrentar os incidentes.

6. O plano deve ser atualizado e testado no mínimo uma vez ao ano e sempre que prestador identificar mudanças no seu ambiente ou sistema que possam gerar riscos em segurança da informação.

Artigo 8.º

**Política de pessoal**

1. O prestador qualificado de serviço de confiança deve adotar as seguintes regras de seleção e contratação dos seus funcionários que reforcem e respeitem as disposições de segurança exigidas para o exercício da sua atividade:

   *a)* Para funções de gestão da infraestrutura que dá suporte aos serviços de confiança, emprega pessoal especializado com conhecimentos específicos em assinatura

eletrónica, certificação digital e outras tecnologias que digam respeito aos serviços prestados, bem como em segurança da informação e privacidade de dados pessoais;

*b)* Todo o pessoal que desempenha funções relacionadas com os processos que dão suporte aos serviços de confiança está livre de conflitos de interesse que possam prejudicar a sua imparcialidade;

*c)* As funções relacionadas com os processos que dão suporte aos serviços de confiança não são desempenhadas por pessoas que se encontram em situação indicadora de falta de idoneidade;

*d)* No âmbito da sua estrutura organizativa contempla, pelo menos, os seguintes cargos e funções necessários à operação dos sistemas que dão suporte aos serviços de confiança:

*i.* Administrador de sistemas: autorizado a instalar, configurar e manter os sistemas, tendo acesso controlado a configurações relacionadas com a segurança;

*ii.* Operador de sistemas: responsável por operar diariamente os sistemas, autorizado a realizar cópias de segurança e reposição de informação;

*iii.* Administrador de segurança: responsável pela gestão e implementação das regras e práticas de segurança;

*iv.* Auditor de sistemas: autorizado a monitorar os registos de atividade dos sistemas;

*v.* Administrador de registo: responsável pela aprovação da emissão, suspensão e revogação de certificados, quando o prestador qualificado de serviços de confiança emitir certificados e selos digitais.

2. Os postos de trabalho ou funções, referidos nas subalíneas *i*), *iii*) e iv) da alínea *d*) do número anterior, não podem ser executados pela mesma pessoa.

Artigo 9.º

**Plano de cessação de atividades**

1. O prestador qualificado de serviços de confiança deve ter um plano de cessação de atividades atualizado, informando que antes de terminar os seus serviços, adotará as seguintes providências:

a) informará do término: todos os assinantes e outras entidades com as quais o prestador tem acordos ou outra forma de relações estabelecidas, entre as quais as partes confiantes, os prestador de serviços de confiança e as autoridades relevantes, como os órgãos de supervisão;

b) terminará a autorização de todos os subcontratantes para atuar em nome do prestador na execução de quaisquer funções relacionadas com o processo de emissão de *tokens* de serviço de confiança;

c) transferirá obrigações para uma parte confiável para manter todas as informações necessárias para fornecer evidências da operação do prestador por um período razoável, a menos que possa ser demonstrado que o prestador não possui nenhuma dessas informações;

d) destruirá ou retirará de uso suas chaves privadas, incluindo cópias de backup, de forma que as chaves privadas não possam ser recuperadas;

e) tomará providências para transferir o fornecimento de serviços de confiança prestados a seus clientes existentes para outro prestador.

2. O prestador qualificado de serviços de confiança deve ter um acordo para cobrir os custos para cumprir estes requisitos mínimos no caso de entrar em falência ou, por outras razões, não conseguir cobrir os custos por si só, na medida do possível dentro dos condicionalismos da legislação aplicável em matéria de falência.

3. O prestador deve declarar nas suas práticas as disposições tomadas para a cessação do serviço.

4. O prestador manterá ou transferirá para uma parte fiável as suas obrigações de disponibilizar a sua chave pública ou os seus *tokens* de serviço de confiança às partes interessadas por um período razoável.

Artigo 10.º

**Dispositivos e sistemas fiáveis**

1. O prestador qualificado de serviço de confiança deve utilizar sistemas e dispositivos fiáveis para a realização das suas operações, com as seguintes características:

*a)* Os Dispositivos Seguros de Hardware, *HSM,* a utilizar para as operações que envolvem chaves criptográficas, devem preencher os seguintes critérios:

*i.* ter garantia de EAL 4 ou superior, de acordo com a norma ISO/IEC 15408, ou critérios de avaliação equivalentes reconhecidos nacional ou internacionalmente para a segurança de TI, desde que esse seja um alvo de segurança ou perfil de proteção que atenda aos requisitos dos documentos aplicáveis ao serviço prestado, com base em uma análise de risco e levando em conta medidas de segurança físicas e outras medidas de segurança não técnicas; ou

*ii.* atender aos requisitos identificados na ISO/IEC 19790 ou FIPS PUB 140-2 nível 3 ou FIPS PUB 140-3 nível 3.

*b)* Os dispositivos criptográficos seguros devem ser operados em sua configuração, conforme descrito na documentação de orientação de certificação apropriada, ou em uma configuração equivalente que atinja o mesmo objetivo de segurança.

*c)* Os Dispositivos Qualificados de Criação de Assinaturas/Selos Eletrônicos (QSCD), fornecidos pelo prestador para os titulares, no âmbito dos serviços de emissão de certificados digitais, e quando aplicável.

*d)* Os algoritmos e parâmetros criptográficos utilizados nas diferentes operações e serviços executados pelo prestador qualificado de serviços de confiança devem refletir com especial atenção a durabilidade dos esquemas de assinatura relativamente à sua resistência a ataques, uma vez que isso afeta diretamente o período de validade que se pretende atribuir aos certificados e assinaturas criados.

*e)* Para tal, devem ser utilizadas as recomendações do Capítulo 8 do documento ETSI TS 119 312 considerando sempre a sua versão mais recente.

*f)* Os sistemas utilizados na execução dos processos críticos, devem ser confiáveis e atender, no mínimo, os requisitos 7.4-04 a 7.4-10 do documento ETSI EN 319 401.

2. Os requisitos para os sistemas confiáveis podem ser garantidos usando, por exemplo, sistemas em conformidade com o CEN TS 419 261, CEN EN 419 241-1 ou com um perfil de proteção adequado (ou perfis), definido de acordo com ISO/IEC 15408.

Artigo 11.º

**Entrada em vigor**

O presente regulamento entra em vigor no dia seguinte ao da sua publicação.